Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 387 – 394

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

A Review on Security Related Aspects in Vehicular Adhoc Networks

Navjot Kaur[a*], Sandeep Kad[b]

[a]*M.Tech Scholar, Department of CSE, Amritsar College Of Engineering and Technology, Amritsar*
[b]*Associate Professor, Department of CSE, Amritsar College Of Engineering and Technology, Amritsar*

Abstract

Vehicular Adhoc Network is a special form of the Mobile Adhoc Network which has received remarkable attention with the growing era. It is capable of providing data communication between the mobile vehicles. It focuses on safety related applications and Internet accessing related applications. The basic model of the VANETs consists of On Board Units (OBUs) and Road Side Units (RSUs). These units communicate through an open wireless medium, creating a threat to the network. As the malicious node can attack the privacy information such as the user's identity, tracing preferences etc., if the node is not properly protected. Therefore, there is a need of security requirements to secure it. The paper describes various requirements, characteristics, challenging issues and techniques of security in VANETs. In this paper a theoretical analysis of different security techniques of Vehicular Adhoc Networks has been done which compare different schemes at different levels like hardware, authentication, privacy and certification techniques etc.

Peer-review under responsibility of organizing committee of the ICISP2015

*Keywords:*Adhoc Networks; Vehicular Adhoc Networks; Security; Authentication; Confidentiality; Non-Repudiation; Trusty Data.

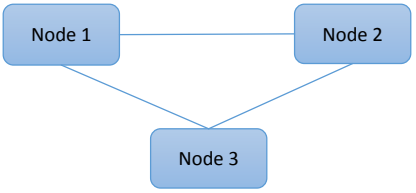
1. Introduction

A wireless ad-hoc network is a distributed type of network. It allows communication between the Vehicular nodes. The network is Adhoc because it does not rely on any infrastructure, such as routers in wired networks or access points in wireless networks. Instead, each and every node participate in forwarding data to other nodes, and so the determination of which nodes forward data can be made at run time to provide network connectivity17. . Moreover these vehicular nodes rely on each other to keep the network connected. Adhoc network is a collection of nodes that is connected through a wireless medium with rapidly changing topology[4-22] .

*Corresponding author. Tel.: +91-855-792-0105;
*E-mail address:*kaur.navjot30590@gmail.com

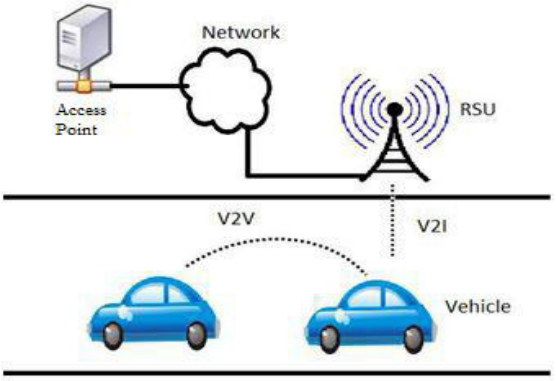
Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.079

Fig.1. Structure of Adhoc Network



With the deployment of the mobile Adhoc communication, and the internet, vehicular Adhoc network has received a remarkable attention from the academia, industry and the government[6] .Vehicular Adhoc network is the subset of the Mobile Adhoc Network[2]. VANETs are a futuristic technology which allows the network of moving the smart vehicles. It takes the moving cars as the nodes in order to create the mobile networks. The participating cars can act as a wireless router or nodes. These participating cars can provide communication between vehicle to vehicle and between the vehicles and the infrastructure[7]

Fig.2.Vehicular Adhoc Network



The connection between the cars is possible approximately up to 100 to 300 meters. When these nodes fall out of the range then a drop out in a network can occurs[7] Figure 2 shows mainly two types of units i.e., OBUs and the RSUs. OBUs is a VANET component which allows the communication among V2V and V2I[20] These units are mounted on the vehicles. Whereas RSUs allows these mobile vehicles to send traffic related information, authentication related information, multimedia messages related information and etc[21] .These units are road aside and are connected to the application servers[13]

VANETS improve the driving experience, traffic safety, multimedia information and entertainment[26] VANETS allows the vehicles to transfer messages with each other and with RSUs One of the emerging and challenging areas in VANETs is security. VANET is the subset of MANET, however it has many aspects different from that of MANET i.e., high mobility of nodes and dynamic topology changing[2] . In Vehicular Adhoc Networks, security of vehicles should be maintained during data transmission.

.1.2 Characteristics of VANETs

Given below are some of the characteristics of Vehicular Adhoc Network:

- *High Mobility and Dynamic changing topology:* Vehicles move in high speed. They can communicate and transmit data usually when they are close to each other that is approximately 300 meters. When vehicles move out of the range then a drop out/ breakdown in a network can occur[1-4]
- *Available Geographic Position for Vehicles:* Vehicles either static or dynamic are equipped with the geographical positioning system such as the GPS systems which helps to provide location aware information[4].

- *Delay Constraint:* In application such as collision warning, network breakdown, pre-cash sensing, etc the network may experience delay constraint. The delay usually occurs when the receiving vehicular node is expected to receive information[4].
- *Mobility Prediction and Modelling for Vehicles:* The movement of vehicles is basically on the pre-defined paths, such as highway, roads, streets etc. This moment of the vehicles helps the other vehicles to predict their nearby locations[4]
- *No Power Constraint:* As we know that in VANETS moving cars are the nodes instead of the handheld device. So, the constraint of the power can be completely neglected because they have rechargeable batteries[4].
- *Quality of Service (QOS*): Quality of service refers to the ability of providing better service to the network over various applications and various topologies.

1.2 Requirements for VANETs

Before deploying the security related system we must satisfy some of the security related requirements. A security related system must fulfil the following requirements:

- *Authentication:* We have two types of nodes i.e., malicious node and genuine nodes, which generate messages in VANETs. Authentication assures that the message is originated by the genuine user. It distinguishes between both the nodes. A vehicular node will block the information send by the malicious node by having an authenticity check. Therefore it can be said that checking the authenticity of the vehicles is very important for securing network[1,4,10,24]
- *Integrity:* Sometimes it happens that the malicious nodes seem to be a genuine one even though it contains some false data. This is because the data received is the same as the data send. The false data is the modified data which can cause crashes, bottlenecks in the network, and other safety related problems. So, integrity must be provided in Vehicular Adhoc Network
- *Availability:* Availability means that each mobile node in the network should be efficient enough of sending any information at any time. It holds the information that is available to the legal/ genuine users. For example: availability of channel should be supported when the channel is under attack such as the DOS attacks or channel jamming[1,4,10,24]
- *Privacy:* The privacy of the node against the malicious node must be guaranteed i.e., the individual and private information of the vehicle should not be disclosed. This will help to reduce the attacks to the system. The malicious node should not be able to avail the vehicles personal information. Therefore at certain degree the identity of the vehicle must be maintained while sending the information or while receiving the information. Preserving users' privacy is mainly related to avoiding disclosure of their real world identities and location aware information[8,10,15,24].
- *Data Verification:* It is essential to verify the data which is to be transmitted among the nodes. Data verification helps to eliminate the false messaging or the malicious node attack[10]

1.3 Applications for Vehicular Adhoc Network

We need to understand the applications of VANETs if we want to design a new effectively running secure system. VANETs applications has be classified in different ways. In addition to that classification method proposed has classified vehicular networking applications into the following three categories[10] :

1.3.1 Safety Related Applications:The road safety applications are used to increase the safety on road. They can further be categorized as[10]

- *Collision warning/Avoidance:* Data transmitted from the RSU to the vehicles may warn the driver of the node that it is not safe to enter in an intersection or divergence. This can prevent the accidents, save many lives and prevent lives from any kind of injury. Finally it will lead in reduction of accidents.

- *Cooperative driving:* The drivers can get the signals for traffic related warnings such as the violation warning, conflict turn warning, wrong way driving warning etc. This can reduce a number of accidents.

1.3.2 User Related Applications: These are the applications that include infotainment i.e., information and entertainment. The user related applications are as follow[10] :

- *Payment services:* Payment services can be utilized to collect toll taxes and it also helps to reduce the wait time and velocity while passing through the toll collection
- *Location aware services:* This is the type of the application that helps the driver to location the nearby restaurant, nearby gas station, or we can simply say to inform the driver about the place of interest. In fact it has been seen that recently many GPS system are already providing us with this type of service.
- *Internet Connectivity:* In today era, people always want to stay connected with the Internet at every place and at every time. Hence in vehicular Adhoc network constant connectivity is provided to the user, so that he/she remain connected with the internet.

1.3.3 Peer to peer application: In vehicular Adhoc network, these type of application are useful to provide services to the vehicles such as the music sharing, movies sharing and downloading, file sharing, audio and video clip etc. among the vehicles in the network.

1.4 Techniques for securing VANETs

VANETs can be secured by using various techniques such as hardware, authentication, privacy and certification techniques etc. Given below are some of them:

- *Hardware Security:* Among all the hardware components there are two specific components that can achieve security in the VANET i.e., a) Event data recorder (EDR), it track all the occurrences of the event. b) Temper proof devices (TPD) are the independent devices and helps to generate and receive the encrypted messages. Hardware security techniques use conventional cryptographic protocols to provide security. Hardware needs to be protected since its insecurities can facilitate attacks on the programs and contents running on it[10] . There are some hardware based threats which are as follow[14-20]. a) *Hardware Trojans*: An attacker either in the design house or in the foundry may add malicious circuits or modify existing circuits. b)*IP piracy and IC overbuilding*: An IP user or a rogue foundry may illegally pirate the IP without the knowledge and consent of the designer. A malicious foundry may build more than the required number of ICs and sell the excess ICs in the gray market. *c)Reverse engineering (RE)*: An attacker can reverse engineer the IC/IP design to his/her desired abstraction level. He can then reuse the recovered IP or improve it.

- *Authentication:* Authentication is a process which justifies the identity of a User who wishes to access it. Since Access Control is normally based on the identity of the User who requests access to a resource. One of the fundamental function of the vehicular communication is to authenticate the sender of the data. The widely used technique for authenticating the messages is to sign the message and then verifying it. Authentication can be providing using encryption along with cryptographic hash function, digital signature and certificates 10. . There is no central authority, and it is much more difficult to authenticate an entity 1. . Vehicular Adhoc Network (VANET) has evolved to complement Intelligent Transportation System (ITS) for communicating safety messages while driving on the road[1] .

- *Detection and Correction of Malicious Data:* When data is allowed to be send between different nodes of a network, the intruders can easily arrange to send false data in valid messages in order to breakdown or jam the network. So it has become an important issue to secure the message. The false data need to be verified. It is not only must to detect whether the sender of the data is genuine or not, but also the data itself is a genuine or not. As from our previous study it is known that Vehicular Adhoc networks rely heavily on node-to-node communication, allowing malicious data traffic. At the same time, the easy access to information in a network by VANETs enables the difficult security goal of data validation to be approved[10]

- *Public Key Infrastructure:* Vehicular public key infrastructure act as a certificate authority (CA). It issues certified public and private keys to each node of the VANET. The vehicle private key must be stored with the encrypted message. The vehicle will sign the message with its own private key at the sender side and adds a CA certificate. The receiver side will obtain the public key of the sender and then will verify the

message. For this the receiver should have a public key of the CA 10. . The purpose of a PKI is to generate secure electronic transfer of information between a range of network activities such as e-commerce, internet banking and confidential email. Public Key Infrastructure is required for activities where simple passwords and proofs is required to confirm the identity of the parties which are involved in the communication and where there is information to validate the information that is to be transferred 24. .

- *Group Signatures:* Group Signature is usually range based. The node that has some attributes in common form the group. Each time the vehicles enters this group, the group private key needs to be changed and transmitted to the new joining node. It allows the group members to sign without disclosing their identities. Only the genuine authority can reveal the identity of the signer[10] .Group signature in VANET is widely used for vehicles to achieve authentication since it allows any of the group member to sign the message on behalf of the group without disclosing its identity. Only the genuine authority can reveal its identity. On receiving a message from an unknown entity or malicious node, a vehicle has to check its certificate so as to avoid communicating with revoked vehicles[3,15].
- *Certificate Revocation:* In public key infrastructure it is necessary to issue the keys. But sometimes it also become necessary to revoke the keys. For example, if the PKI detects that the vehicle is sending an incorrect or false information, then it becomes necessary to revoke it. Revocation list maintains the record of all the revoked list. The reason behind the revocation is that the user no longer has the private key (e.g., it may be happen because the token containing the private key has been lost or stolen)[10].

2. Related work

Chaurasia et al[3] proposed a scheme based on group signature of continually transmitting of mobile vehicles. As in mobile vehicles the moment of vehicles is dynamic that is they send and receive messages on road. this type of communication creates a threat to the in information and identity of vehicles. So this paper provides a scheme to broadcast a message by preserving its security, anonymity. Yeongkwun et al[10] proposed that Vehicular Adhoc Network plays an effective role for improving traffic Management and safety. It also focus on wide range of value added services such as collision Warning/ Avoidance. As information transmitted over Vehicular Adhoc Network is highly sensitive and is important for safety discussions, safety requirement applications. However it is important to have security and privacy of vehicles. Security and privacy are the two important aspects that encourage the VANETs design. This paper outlines some of security solutions for threats and attacks to the moving Vehicular nodes. Xiaoyan et al[26] proposed an efficient privacy preserving authentication scheme based on group signature for Vehicular Adhoc Networks (VANETs). In our scheme, we first divide the whole area into several domains. In it road side units (RSUs) are responsible for distributing group private keys and managing vehicles in a localized scenario. The Hash Message Authentication Code (HMAC) is used to restrict the time-consuming CRL checking, so as to ensure the integrity of messages before batch group authentication. It also contains cooperative message authentication which each vehicular node just needs to verify a small number of messages, so as to reduce authentication burden. Vanita et al[17] focus on the detail study of Adhoc network, its protocols and different types of networks in. VANETs is a blowing field which places lot of attention on networking. VANETs has the property of dynamic mobility which means nodes can move from one place to another place, within its network and any node can join the network and can leave the network at any time. Mobile Nodes can be in the form of systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. At same time these dynamic nodes can look like host/router or both. Security is an immediate and earlier solution to this. Rong et al[2] proposed a cluster-based scheme which can be applied in VANET for transmitting data, It discusses the cluster head (CH) selection algorithm and a cluster switching algorithm for VANET. The proposed CH selection algorithm combine considers node degree, the available resource of candidate CHs and the velocity difference between candidate CHs and other cluster members (CMs) in a present cluster. It proposed optimal cluster switching scheme that focuses on QoS requirements of both delay-sensitive service and throughput-sensitive service. Thus improving the security. Chirag Suyakant et al[22] proposed a mechanism for content sharing between vehicle-to-vehicle communications so as to help the users find their interested content on the road. VANETs provides peer-to-peer content distribution of data items for traffic related information, audio, video and other such information. Reliability, security and fast communication are the desperate need in VANETs for inter-vehicular communication. In this paper a model is considered which satisfies the

presented parameters. Kakkasageri et al 11. proposed a paper that is mainly concerned with the safety related applications such as reliability, security, trust, real time delivery and latency. it also includes gathering, aggregation, validation and dissemination of information in VANETs. Mario Gerla et al 7. shows the state the art of technologies and protocols for content distribution in VANETs. It considers some of the main challenges i.e., Internet access spectrum scarcity, mobility, connectivity intermittence and scalability. Other Aspects covered in it include: coexistence of Wi-Fi and LTE; application of network coding; protection from pollution attacks. Atanu et al 13. controls channel congestion dynamically by reducing the rate of messages to be transmitted among vehicular nodes. The rate of transmitting the messages can be decreased by restricting the attackers and by decreasing the channel load and allowing only the authentic messages to flow so that they can be availed in a network. This paper highlights how the performance of channel congestion can be controlled with and without attack. Shital et al 4. proposed secure and reliable content distribution in VANET. VANET has been an open medium for passing the packet data. Due to open medium there is less security in content distribution and as well as less reliability in content distribution while using broadcasting protocol. Neeraj et al 16. proposed a work of a CCDSV that builds cooperative APs into a hybrid structure called the contact map which is based on the vehicular contact patterns observed by APs. The selection process takes AP's storage capacity, storage status, inter-APs bandwidth and traffic loads. Network coding is also applied in CCDSV to enhance the distribution of shared contents. The paper, introduces a system that takes advantage of the RSUs that are connected to the Internet and providing various types of information to VANET users. Mamun et al 12. proposes an application friendly scheme which is the combination of the linking, direct opening, Message dependent opening, revoking batch verification in a single scheme of GS. It informs whether the message is coming from the same messenger. It does not include the opener of the message.

3. Challenging issues for Vehicular Adhoc Networks

There are various challenges that can be discussed for vehicular wireless network. Some of them are discussed below 9,13. :

3.1 Technical Challenges: The technical challenges deals with the technical barriers such in network management, congestion and collision control, environmental.

- *Management of Network:* Due to dynamic and high mobility, nature of VANETs, it is difficult to manage the network. Whenever a vehicular node changes its path, its neighbouring vehicles also change, which give rise to the formation of the new network scenarios.
- *Congestion/collision Control:* During the rush hours i.e., when the network is heavily loaded, the chances of collision and congestion in the network is more. So, it becomes essentially important to reduce the network load.
- *Security:* Among all the challenging issues Security is one of the major challenge that can be considered in each and every network. During the data transmission, the data is transmitted in an open medium. The data can be any form such as files, movies, audio or video clip etc. So, when any of the malicious node sends the false data in a network it can cause the breakdown in the network. Therefore it is important to secure data at the sender side and the receiver side.

3.2 Social /Economic Challenges: Except from the technical challenges, social and economic challenges can also be taken into notice. Because it is hard to convince the users with such kind of monitoring and new technique 18. .

3.3 Data management and storage

If at a large scale a number of vehicles needs to communicate with each other, then the data need to be distributed and also stored somewhere. This was noted in 25. . So this is a new and unique challenge for massive distribution and storage.

3.4 Tracking for destination

In Location based vehicles, our major concern is communication. Here tracking means creating a path between the nodes by identifying the initial and the next nearby node. Therefore tracking of destination is to reach to the target node from the initial node by identifying the next-next node. So, tracking of destination is also major challenge 23. .

3.5 Co-operative Communication

Co-operation among the vehicles is also necessary as it helps the user to know about various traffic conditions, weather conditions and routes between the vehicles. Such type of communication helps the user to know that up to which extend the information can be shared 19. .

4. Theoretical Analysis

The table below shows the theoretical analysis of various techniques of VANETS. It differentiates these techniques from each other by highlighting the advantages, disadvantages and level of security between them

Table 1: Theoretical analysis on different security techniques

Technique	Year of develop	Advantages	Disadvantages	Level of Security
Hardware Security	2008	Use cryptography protocols	Programs and content running on it is not secure	Hardware level
Authentication	1984	Use encryption, hash function, digital signature and certificates	Difficult to authenticate an entity	Authentication level
Detection and correction of Malicious Data	2004	Node to node communication	Passive node attack	Data level
Public key Infrastructure	2010	Private key is kept with encrypted message	Malicious node can access the public key of the sender node	Certificate Authority
Group Signature	1991	Any group member can sign the message	Any attacker node can access the information of group	Group Based
Certificate Revocation	2010	Maintains the record of all revoked keys	User no longer possess the private key	Certification Based

5. Conclusion and Future scope

Securing of information is the main point of concern in the recent era as a large number of messages are transmitted. Also VANETs provide a dynamic open medium for information flow. The attackers can cause a threat to it due to its wireless nature. Therefore a secure way should be adapted. From the above discussion, some of the important issues that can be taken into notice are:

- A smart vehicular system is needed to be designed so that the vehicles are able to understand, route and process the information to the other vehicles.
- Vehicles need to process secure and optimized information.
- Only the authenticated and genuine mobile vehicular nodes must receive the information.
- A certain range must be set between the vehicles so that the secure information can be accessed more easily and in a secure manner.

Among all the challenging issues security is one of the major challenges that can be considered in each and every network. This paper theoretically analyses the performance of different security methods in VANETs techniques such as hardware, authentication, privacy, PKI, group signature and certification techniques. It also discusses the various characteristics and challenging fields in VANETs. Various security based techniques are discussed in this paper and it is observed that these schemes still fails because of trust factor which is not easy to measure. So, it is concluded that still there is a scope of security in VANETs. In future a high level improvement of security based approach is needed to be developed for more secure environment which helps to prevent network from various attacks.

References

1. Bhosle A., Pandey Y. Review of authentication and digital signature methods in Mobile Adhoc network. *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 2(3), pp. 1220-1224, 2013.
2. Chai R., Yang B., Li L., Sun X., Chen Q. Clustering-based Data Transmission Algorithms for VANET. *IEEE*, 2013.
3. Chaurasia B., Message broadcast in VANETs using Group Signature *IEEE*, pp. 131-135, 2008.

4. Chauhan S., Patel H. Secure and Reliable Content Distribution in VANET *International journal of scientific Research & Development*, vol. 2(3), pp. 2321-0613, 2014.
5. Dak A., Yahya S., Kassim M. A Literature Survey on Security Challenges in VANETs. *International Journal of Computer Theory and Engineering,* vol. 6(6), 2012.
6. Feiri M., Petit J., Schmidt R., Kargl F. The Impact of Security on Cooperative Awareness in VANET. *IEEE Vehicular Networking Conference*, pp. 127-134, 2013.
7. Gerla M., Wu C., Pau G. Content Distribution in VANETs. pp. 3-12, 2014.
8. Golle P., Greene D., Staddon J. Detecting and Correcting Malicious Data in VANETs. 2004.
9. Johnson M., Nardis L., and Ramchandran K. Collaborative Content Distribution for Vehicular Adhoc Networks. 2009.
10. Kim Y., Kim I Security Issues in Vehicular Networks *IEEE,* pp. 468-472, 2013.
11. Kakkasageri M.S, Manvi S.S. Information Manangement in Vehicular Adhoc Network: A Review. *Journal of Network and Computer application,* pp 334-356, 2014.
12. Mamun M. Secure VANET Application with refined group Signature. *IEEE Twelfth Annual conference on Privacy, security and trust* (PST) pp. 199-205,2014.
13. Mondal A., Mitra S. Dynamic and Distributed Channel Congestion Control Strategy in VANET. *International Conference on Advances in Computing, Communications and Informatics (ICACCI), accepted by IEEE*, 2014.
14. Majzoobi M., Koushanfar F., Potkonjak M. Testing Techniques for Hardware Security. *IEEE International Test Conference*, pp. 1-10, 2008.
15. Priya K., Karuppanan K. Secure Privacy and Distributed Group Authentication for VANETs. *IEEE,* pp. 301-303,2011
16. R.M.E N., Jebakumari M. An Effective Secure Mechanism for Vehicular Content Distribution in VANET. *International Journal of Computer Trends and Technology,* vol. 8(4), pp. 167-172, 2014.
17. Rani V., Dhir R. A Study of Ad-Hoc Network: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering*. Volume 3, Issue 3,pp.135-138, 2013.
18. Radhika S., Sindhu S. A study on security challenges, issues and their solutions for vehicular ad-hoc network (VANET) *International Journal of Multidisciplinary Research and Development*,2015
19. Rehman S., Khan M., Zia T., Zheng L. Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges. *Journal of Wireless Networking and Communications*, pp. 29-38,2013
20. Rostami M., Koushanfar F., Karri R. A Primer on Hardware Security: Models, Methods, and Metrics. *Proceedings of the IEEE*, pp no (1283-1295), vol.102 (8), August 2014.
21. Singh k., Yadav R. A review paper on Adhoc network security. *International journal of computer science& security*, vol 1, pp. 52-69.
22. Thaker C., Garg A., Shafi N. Securing peer to peer content distribution network based on network coding in Vanets. *International Journal of Computer Applications,* vol 66(4), pp. 30-33, March 2013.
23. Thomaidis R., Vassilis K., Lytrivis P., Tsogas M, Karaseitanidis G., Amditis. Target tracking and fusion in vehicular networks. *In Intelligent Vehicles Symposium (IV), IEEE*, pp.1080 –1085, 2011
24. Wasef A., Lu R. Complementing Public Key Infrastructure to Secure Vehicular Adhoc Networks. *IEEE Wireless Communications,* pp. 22-28, 2010.
25. Wolfson O., Xu B., Cho J. Multimedia traffic information in vehicular networks. *In Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pp. 480–483, 2009.
26. Zhu X., Jiang S., Wang L., Li H., Zhang W., Li Z. Privacy-Preserving Authentication Based on Group Signature for VANETs. *IEEE Wireless Networking Symposium*, pp. 4609-4614, 2013.